ARGUMENTS/REMARKS

Overview

Claims 1-5 and 11–15 remain in the application. No claims have been canceled. No claims have been amended. No new claims have been added.

The rejection of independent claims 1 and 11 under 35 USC 103(a), as being unpatentable over Bianco[1] in view of Ditto[2] is hereby traversed, and reconsideration thereof is respectfully requested, in view of the reasons and remarks set forth below.

Claims 1 and 11 Are Patentable Over the Cited References

Each of claims 1 and 11 recites, in pertinent part, applying an initialization code to a first chaotic system whose dynamics cannot be determined solely from the initialization code. The initialization code causes the first chaotic system to assume a periodic orbit and generate a first key bitstream. The claims also recite applying the initialization code to a second chaotic system—identical to the first chaotic system—to synchronize the second chaotic system with the first chaotic system. The recited second chaotic system generates a second key bitstream identical to the first key bitstream.

As described in the specification (e.g., at p. 11, last paragraph, and p. 12, lines 1–2) an important advantage of the systems and methods of the claimed invention is the ability to drive a first chaotic system and a second chaotic system onto the same periodic orbit and synchronize them by applying a select initialization code to each of the chaotic systems. As further explained in the specification (p. 3, last line and p. 4, lines 1–2), another important advantage of the systems and methods of the invention is that the actual key is not transmitted; rather, it is generated remotely at the second chaotic system. No information is transmitted from which the encryption key or the chaotic system could be reconstructed.

---

[1] U.S. Patent 5,048,086 (Issued 10 September 1991)
[2] *Introduction: Control and synchronization of chaos*, William L. Ditto and Kenneth Showalter, *Chaos* **7** (4), 1997, pp. 509–511.

Notably, as explained on p. 3, lines 7–9 of the instant specification, even if the initialization code—which is transmitted from the first chaotic system to the second chaotic system—is intercepted, it cannot be used to reproduce the key bitstream or the chaotic system, without knowledge of the dynamics of the chaotic systems.

In fact, not every bitstream can serve as an initialization code. For example, as the instant application states, only "certain controls may be used as initialization codes." (p. 5, lines 4–5). More particularly, as stated on p. 12, lines 11–18:

> [It] is possible to send an initialization code to two chaotic systems that drives them onto the same periodic orbit. There are numerous control sequences that, when repeated, lead to a unique periodic orbit for all initial states, so that there is a one-to-one association between a sequence and the orbit. However, for some control sequences the orbits themselves change as the initial state of the chaotic system changes. Consequently, repeated control sequences can be divided into two classes, initializing codes and non-initializing codes.

The cited references, individually or in combination, fail to suggest or teach the recited initialization code and/or uses thereof for remotely generating an encryption key.

Ditto—admitting that his introductory paper is merely a "cursory glance at the field" (Ditto, p. 509, col. 2, line 2)—reports second hand on what he believes certain parties are doing in the art of control and synchronization of chaotic systems. In particular, Ditto states that "carefully chosen, tiny perturbations" can "be used for stabilizing virtually any of the unstable periodic orbits making up a strange attractor." (Ditto, p. 509, col. 1, lines 8–10). However, Ditto fails to teach *what* these "carefully chosen, tiny perturbations" are, *how* they are produced, and *how* they are applied to a chaotic system to drive it onto a periodic orbit. Ditto also reports second hand, and quite briefly, that Cuomo[3] employs synchronized chaotic systems in a scheme for private communication." (Ditto, p. 509, col. 1, lines 43–46).

---

[3] *Circuit implementation of synchronized chaos with applications to communications*, K. M. Cuomo and A. V. Oppenheim, *Phys. Rev. Lett.* **71**, 65–68 (1993).

However, nowhere does Ditto teach or suggest using the recited initialization code, or an equivalent thereof, to drive a first chaotic system onto a periodic orbit and applying the initialization code to a second chaotic system to synchronize the second chaotic system with the first chaotic system. Moreover, Ditto's cursory reference to chaos-based secure communication systems and methods is limited only to the work of Cuomo.

On 4 February 2004, Applicant submitted remarks and arguments in response to a Non-Final Office Action (dated 11 September 2003, Paper No. 5), describing the deficiencies of Cuomo and distinguishing the claimed subject matter of the instant application therefrom. In response to the Examiner's suggestions to recite certain limitations in the claims, Applicant submitted, as part of a Request for Continued Examination (RCE) filed on 26 October 2004, amendments, remarks, and arguments further distinguishing the claimed subject matter from the teaching of Cuomo. The Examiner, citing new references, declared the arguments and remarks moot, and did not reply to the specific points raised by Applicant.

Given that Ditto, one of the new references cited by the Examiner in the last Office Action, specifically points only to Cuomo in discussing use of chaotic systems for private communication, Applicant respectfully requests that the Examiner either specifically address Applicant's remarks and arguments—set forth previously and presented below to distinguish the claimed subject matter from the teaching of Cuomo (cited by Ditto)—or withdraw the rejection of the claims.

Cuomo teaches using a "drive signal," but Cuomo's "drive signal" is not equivalent to the recited initialization code. Unlike the recited initialization code, which, as described on p. 3, lines 7–9 of the instant specification, reveals no information about the chaotic system to which it is applied, Cuomo's "drive signal" is a chaotic signal that reveals information about the state and dynamics of the chaotic system.

Cuomo employs what is commonly referred to as additive chaos masking. The message signal is embedded in the data that Cuomo transmits to a receiver for decryption. A known drawback of additive chaos masking is that an attacker can

infer the dynamics of the first chaotic system, determine the masking signal, and subtract the masking signal from the transmitted information to reveal the masked message signal. As the systems and methods of the instant application employ an "initialization code," not a chaotic "drive signal," and do not transmit the message signal, no such dynamic information can be inferred from what is transmitted between the first and second chaotic systems.

Also in response to the Office Action dated 11 September 2003, Applicant submitted a Supplemental Information Disclosure Statement (IDS) which included a paper titled "A Survey of Chaotic Secure Communication Systems," by Tao Yang. Yang describes the chaotic signal masking approach of Cuomo (see Yang, p. 84, first paragraph of section 2.1, and p. 85, Fig. 1(a)) and discusses the drawbacks of Cuomo's system and method (see Yang, p. 88, second paragraph). In particular, Yang cites a paper by Kevin M. Short (Applicant), titled "Steps Toward Unmasking Secure Communications" (included in the same IDS submission). Both of these papers further discuss how—in contrast with the initialization code recited in claims 1 and 11—subtracting Cuomo's masking signal from the transmitted information reveals the masked message signal.

Bianco fails to remedy the deficiencies of Ditto (and Cuomo). Bianco teaches an encryption system and method at the core of which is a nonlinear equation that exhibits chaotic behavior when properly initialized. For example, Bianco uses a class of nonlinear equations prototypically represented by the logistic difference equation, $x_{n+1} = \mu x_n(1 - x_n)$, which he asserts exhibits chaotic behavior for certain values of the tuning parameter μ and certain initial conditions. The nonlinear equation produces a sequence of iterates x_n having floating-point values.

Bianco applies a transformation to the sequence of iterates to convert it to a binary keystream. As shown by block 27 of Bianco's FIG. 1, Bianco sums the binary keystream with the message signal. This is also shown in the adder block 64 of Bianco's FIG. 3, wherein the message is added to the keystream to produce a masked message signal called a ciphertext. The ciphertext is then transmitted from the encryptor to the decryptor.

Bianco's chaotic signal masking system and method have drawbacks substantially similar to those of Cuomo. Therefore, arguments distinguishing the subject matter claimed in the instant application from Cuomo's signal masking system and method also apply to the signal masking system and method of Bianco.

It is at least in part this type of prior art deficiency that the recited use of an initialization code in each of claims 1 and 11 avoids by generating the key at the second chaotic system and not transmitting the key (nor anything from which the key or the dynamics of the chaotic systems can be inferred) from the encryptor to the decryptor.

Bianco also teaches that his system and method rely critically on (1) sensitive dependence of the chaotic system on initial conditions and (2) aperiodic behavior of the chaotic system. For example, he states (col. 2, line 66 to col. 3, line 7):

> Chaotic behavior may be described as a form of steady state behavior which is aperiodic and as such appears to have noise-like characteristics. This behavior, although aperiodic, is bounded, and while the chaotic trajectory never exactly repeats itself, the trajectory is completely deterministic given the exact initial conditions and parameter values. These chaotic properties are used to generate an aperiodic sequence for use as the keystream in the encryption system of the present invention.

Bianco further suggests that increased aperiodicity of the sequence of iterates generated by his chaotic system results in stronger encryption (col. 3, lines 44–47; col. 3, lines 55–57; and col. 4, lines 5–7):

> It has been mathematically proven that operation in the chaotic region will produce an aperiodic sequence, making it appear as if an infinite cycle length can be obtained ... In practice, however, the floating-point precision of the machine implementation determines the maximum cycle length that is available ... [E]xtremely long cycle lengths can be obtained by simply increasing the precision of the implementation.

Bianco essentially views the finite precision floating-point arithmetic imposed by practical computing hardware and software as an unwanted limitation. He suggests using higher-precision computing hardware and software to mitigate the periodicity (finite cycle length) imposed by finite-precision arithmetic capabilities of practical computing hardware and software, thereby improving encryption security.

In other words, Bianco teaches away from driving the chaotic system onto a periodic orbit. A periodic orbit produces a periodic sequence of iterates which would be at variance with the teaching of Bianco. This is in contrast with the recited subject matter of the claims in the instant application, wherein the initialization code tames aperiodic tendencies of the chaotic system, drives it onto a periodic orbit, and in fact stabilizes the otherwise unstable periodic orbit, regardless of the initial state. As Bianco teaches away from driving the chaotic system onto a periodic orbit, it cannot be combined with Ditto or any other reference that may teach driving a chaotic system onto a periodic orbit.

Furthermore, as mentioned above, exploiting a chaotic system's sensitive dependence on initial conditions is critical to Bianco's system and method. Bianco relies on the fact that "totally different keystreams [are] obtained from minor changes to the initial conditions." (col. 7, lines 4–5).

Bianco teaches that a random starting point is created—signifying the initial value of x_n. The nonlinear equation at the encryptor is then iterated for an amount equal to the "run-up" value specified in a "cryptographic key" to determine the initial starting point. The initial value x_n is prepended to the encrypted message (masked signal) and is sent to the decryptor, along with other components of the cryptographic key such as the "run-up" value.

The recursive nonlinear equation at the decryptor is supplied the initial value and the run-up value (see items 20 and 40 in Bianco's FIGS. 1 and 2, respectively) and is allowed to iterate to produce new iterate values. As Bianco states, this causes the decryptor to deterministically generate an extremely large number of uniformly-distributed iterates, thereby allowing the "decryptor to easily obtain synchronization with the encryptor." (col. 4, lines 11–14).

As Bianco teaches that his decryptor easily synchronizes with his encryptor, there is no motivation to combine Bianco with any other reference that may teach an alternative way of synchronizing two chaotic systems. This provides additional support against combining Bianco with another reference that may teach synchronizing two chaotic systems by driving them onto identical periodic orbits.

The critical reliance on sensitivity of his encryptor and decryptor on initial conditions detracts from any motivation to combine Bianco with another reference to teach the initialization codes of the instant application (which can drive the recited chaotic system onto a periodic orbit *regardless* of the initial conditions). To teach the recited initialization codes of the instant application necessarily reduces the importance of the initial conditions, and therefore interferes with the functional purpose of the parameters in Bianco's cryptographic key which exploit the criticality of those initial conditions. As stated earlier, Bianco's nonlinear equation's chaotic behavior depends at least in part on proper initial conditions.

As stated in the MPEP, 2143.01, a proposed modification cannot change the principle of operation of a reference. Nor can a suggested combination of references require a substantial reconstruction and redesign of the elements shown in the primary reference as well as a change in the basic principle under which the primary reference construction was designed to operate. No combination of references can include Bianco and still teach the recited subject matter of claims 1 and 11, without substantial modification to Bianco's system and method. Accordingly, such a combination is not allowed.

For at least the reasons that neither Bianco nor Ditto, nor any combination thereof, teaches or suggests the recited use of an initialization code, Applicant respectfully requests that the Examiner reconsider and withdraw the rejection of claims 1 and 11. As claims 2–5 and 12–15 variously depend from claims 1 and 11 and recite further limitations thereon, Applicant also respectfully requests that the Examiner reconsider and withdraw the rejection of the dependent claims.

CONCLUSION

In view of the above remarks, Applicant submits that claims 1–5 and 11–15 are in condition for allowance, and requests that the Examiner pass this application to allowance.

If the Examiner believes that a telephone conversation with Applicant's attorney would expedite allowance of this application, the Examiner is invited to call the undersigned.

Dated: 23 March 2005

Respectfully submitted by,

Wolfgang E. Stutius
Registration No.: 40,256
ROPES & GRAY LLP
One International Place
Boston, Massachusetts 02110-2624
(617) 951-7000
(617) 951-7050 (Fax)
Attorney/Agent for Applicant

NOTE: It is believed that fees due in connection with this submission have been appropriately provided. However, if an additional fee amount is due, please charge Deposit Account No. 18-1945, under Order No. CAOT-P02-001, from which the undersigned is authorized to withdraw.